Admin Minnesota
DEPARTMENT OF ADMINISTRATION

Advisory Opinion 12-014

This is an opinion of the Commissioner of Administration issued pursuant to Minnesota Statutes, section 13.072 (2012). It is based on the facts and information available to the Commissioner as described below.

Facts and Procedural History:

On July 30, 2012, the Information Policy Analysis Division (IPAD) received a letter from Matthew Quinn, Chief Deputy County Attorney for Stearns County, dated July 27, 2012. In his letter, Mr. Quinn asked the Commissioner to issue an advisory opinion regarding the use of an automated law enforcement data mapping program in Stearns County and the City of St. Cloud and the program's possible effect on data subjects' rights.

In letters dated August 13, 2012, the Commissioner offered James Miller, Executive Director of the League of Minnesota Cities, and Jeff Spartz, Executive Director of the Association of Minnesota Counties, an opportunity to comment. Both declined to comment.

A summary of the facts follows. Mr. Quinn wrote in his opinion request:

> I am writing to request an advisory opinion regarding the use of an automated law enforcement data mapping program that publishes law enforcement data to the public via a program displayed on the [web]. The program in use in approximately 60 Minnesota municipalities and counties, known as CrimeReports(.com), is being considered for implementation in both Stearns County and the City of St. Cloud, MN.
> …
> CrimeReports combines law enforcement data with a mapping program and an analytics module so that members of the public can view data within a choice of descriptive formats. Put simply, nightly comprehensive law enforcement data is sent from law enforcement's records management system (RMS) and computer aided dispatch (CAD) systems to a CrimeReports server.
> …
> [T]he version of the application that is being considered for implementation – is the publicly viewable version which is proposed to be made available via a link within Stearns County's official website and populated with data from the Stearns County law enforcement RMS. The RMS stores arrest data, request for service data, response or incident data, and criminal investigative data… Other variable parameters that may be searchable in CrimeReports include date ranges which are limited potentially only by the availability of the data in the source database, as well as selected locations including

> cross streets, areas as small as ¼ mile from a landmark (school, park, or major street), within certain boundaries (neighborhood or crime watch area) and also *specific addresses*. It stores other data as well, but the named categories[, which] are the bulk of the data in question here, are regulated by Minn. Stat. [section] 13.82. [Emphasis provided.]

Issue:

Based on Mr. Quinn's opinion request, the Commissioner agreed to address the following issue:

> Would a data subject's rights be violated if certain data about him/her were automatically uploaded to an automated crime mapping system as described above?

Discussion:

Data that law enforcement agencies collect, create, and maintain are classified pursuant to Minnesota Statutes, section 13.82. Certain law enforcement data are always public, certain law enforcement data are never public, and certain law enforcement data may become public depending on the occurrence of certain events or the existence of certain conditions.

Section 13.82, subdivisions 2, 3 and 6, identify law enforcement data that are always public: arrest, request for service, and response or incident data. Inactive investigative data are also public, pursuant to subdivision 7. The data displayed in *CrimeReports* are automatically populated from these generally public data. However, one of the circumstances in which data are never public is when those data qualify for protection under subdivision 17. Subdivision 17 classifies certain identification data as private, including: the identity of a victim or alleged victim of criminal sexual conduct, the identity of a witness or victim of a crime who requests that his/her identity be withheld, the identity of a person who placed a call to the 911 system, the identity of certain juvenile witness, and the identity of individuals required by statute to report certain crimes to the authorities. The government entity is required to evaluate each situation and to exercise its discretion to determine whether an individual's identity qualifies for protection under subdivision 17.

Additionally, Minnesota Statutes, section 260B.171, subdivision 5, provides:

> Except for records relating to an offense where proceedings are public under section 260B.163, subdivision 1, peace officers' records of children who are or may be delinquent or who may be engaged in criminal acts shall be kept separate from records of persons 18 years of age or older and are private data.

Section 260B.171 also requires prior evaluation before determining whether data are private or accessible to the public.

Minnesota Rules 1205.0200, subpart 4, states that data are, "data on individuals" if the data element identifies an individual in itself, or if it can be used in connection with other data elements to uniquely identify an individual. (See also, Advisory Opinion 07-001.) In his opinion request, Mr. Quinn provided corresponding address and homeowner information, which are available to the public on the Stearns County Auditor-Treasurer website, for each of the examples he provided, illustrating how protected identifying information might be inadvertently disclosed. However, when data are sufficiently de-identified, the data are no longer data on individuals and therefore, an entity is not at risk of disclosing private or confidential data.

Mr. Quinn provided three examples of the type of data that *CrimeReports* makes automatically available to the public, including the incident identification information and the corresponding maps.

Example 1:

Incident identification information
Date: 10-10-2011
Address: xxx Block of xxxxx Ave (Stearns County, MN)
Identifier (ICR) Number: ########
CrimeReports displays the call as “Juvenile Problem”

While not publically available, the Computer-aided dispatch (CAD) notes indicate that this call was for the transportation of a child with mental health issues to a hospital via an ambulance. It is not clear in this example whether these data would reveal a protected identity (possibly under section 13.82, subdivision 17(f)), how remote a possibility that might be, or whether the data are sufficiently de-identified. But the County and the City have to make the required determinations about the classification of the data, *prior to* uploading them to *CrimeReports*.

Example 2:

Incident identification information
Date: 10-09-2011
Address: xxxxx Block of CR xxx (Stearns County, MN)
Identifier (ICR) Number: ########
CrimeReports displays the call as “Juvenile-Alcohol Offender”

The CAD notes indicate that this call involved citations for minor alcohol consumption and other concerns related to substance use. The map corresponding to this incident report identifies five houses on the block specified. Assuming that one of the five addresses in the block reveals the juvenile’s residence, there is a slight possibility of disclosing protected data.

Example 3:

Incident identification information
Date: 2-12-2012
Address: xxxxx Block of xxx Road (Stearns County, MN)
Identifier (ICR) Number: ########
CrimeReports displays the call as “Juvenile Problem”

The CAD notes indicate that this incident report was sent to the County Attorney for review of possible felony charges. Section 260B.171 makes data on juveniles private where proceedings about an alleged offense are not public. At the point in time when the data are uploaded from

Stearns County or the City of St. Cloud to *CrimeReports* (apparently, the day the call is reported), it is not necessarily clear whether the incident will be the subject of public proceedings or whether the incident identification information reveals the juvenile's address. Therefore, in this example, there is a possibility that displaying the data may violate that juvenile's rights as a data subject.

These examples also highlight the challenges posed by *CrimeReports*' automated mapping system, especially in rural or less densely-populated areas where the identification of the block and the street could potentially reveal protected data even not in combination with any additional data. (Example 2 involves a block with five houses, but it is entirely plausible that an incident might be reported where there is only one property on the specified block.) In areas where rental housing may be more prevalent or where the population is denser (e.g., more multi-family residences), the risk of identification would likely be lessened.

In many cases, a system displaying data made public by section 13.82, subdivisions 2, 3, 6, and 7, may be appropriate and the risk of revealing a protected identity remote. However, in addition to the examples Mr. Quinn provided, there are other situations where the entity is required by Chapter 13 to exercise discretion, notably the provisions of section 13.82, subdivision 17. For instance, before protecting the identity of a victim or witness who requests protection under subdivision 17(d), the government entity must complete a two-part evaluation. (See Advisory Opinion 01-069.) *CrimeReports* apparently does not have a mechanism to conduct this required evaluation.

The Commissioner opined on an issue similar to the one raised in this opinion, in Advisory Opinion 10-016. There, he stated that the mere possibility that a data subjects' rights might be violated did not preclude disclosure of the data. Rather, an entity's responsibility to respond appropriately to a data request requires that the entity, "must determine, on a case-by-case basis, whether certain data related to an incident must be protected," instead of declining to fulfill the request based on a potentiality. The situation here, though reversed, leads to the same conclusion; the City and the County cannot make all of the specified data automatically public, without first having made the required determinations regarding the classification of the data, however likely or unlikely the risk of inappropriate disclosure. *CrimeReports*, as described by Mr. Quinn, does not appear to allow for those determinations to be made and insofar as *CrimeReports* is unable to do so, data subjects' rights may be at risk.

The Commissioner recognizes the difficulties entities face when attempting to use existing computer programs and web applications as more efficient means of providing access to public data. He agrees that the requirements of Chapter 13 cannot always be adequately addressed by a wholly automated system. However, the limitations of technology cannot relieve a government entity of its responsibility to exercise discretion under Chapter 13. The Commissioner encourages entities to use caution when evaluating how best to use these types of programs, to ensure that the rights of data subjects are not put at risk.

Opinion:

Based on the facts and information provided, the Commissioner’s opinion on the issue Mr. Quinn raised is as follows:

> A data subject’s rights may be violated if certain data about him/her were automatically uploaded to an automated crime mapping system as described.

Spencer Cronk

Spencer Cronk
Commissioner

September 18, 2012